OPIC
OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA

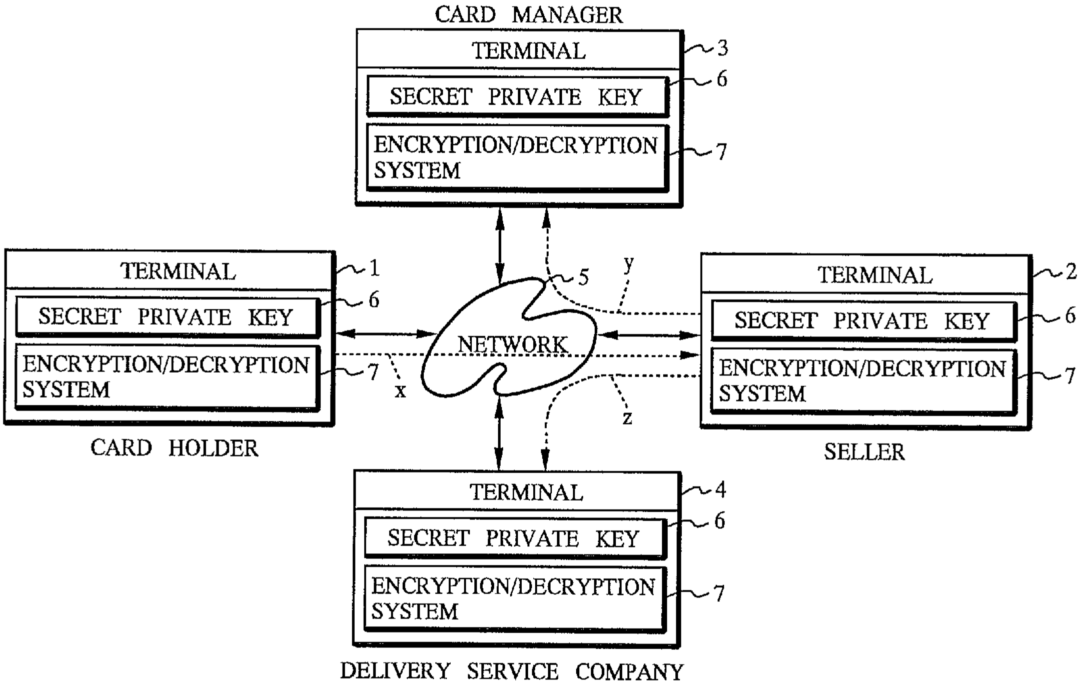
CIPO
CANADIAN INTELLECTUAL PROPERTY OFFICE

(12) (19) (CA) **Demande-Application**

(21) (A1) **2,247,479**
(86) 1997/02/19
(87) 1997/08/28

(72) BABA, Yoshimi, JP
(71) CARD CALL SERVICE CO., LTD., JP
(51) Int.Cl.^{6} G06F 17/60
(30) 1996/02/21 (70834/8) JP

(54) **SYSTEME DE COMMERCE ELECTRONIQUE**
(54) **ELECTRONIC COMMERCE SYSTEM**



(57) Ce système simple de commerce électronique général fait appel à des communications en ligne, à l'aide d'une carte de crédit, sans risque de transaction avec un faux marchand et en garantissant des transactions sûres. Quand un détenteur de carte achète un article à un marchand, le terminal (1) du détenteur chiffre des données partielles concernant les parties y compris le marchand, le gestionnaire de carte et le distributeur recevant les données de la commande, à l'aide d'une clé de cryptage commune efficace seulement entre ces parties, puis il transmet ces données chiffrées aux terminaux (3) et (4) via le terminal (2) du marchand chaque partie procède aux opérations souhaitées en décryptant les données partielles la concernant, en utilisant la clé de cryptage commune utilisable par le détenteur de carte.

(57) A simple, general-purpose electronic commerce system through on-line communication using a credit card without risks of doing a deal with a bogus merchandise dealer, ensuring safe business dealings. When a card holder purchases an article from a merchandise dealer, the card holder terminal (1) enciphers partial data relating to parties including the merchandise dealer, the card manager, and the distribution dealer of the order data, using a common encryption key effective only between the parties and then transmits the enciphered data to the terminals (3 and 4) via the terminal (2) of the merchandise dealer. Each party does its desired business dealing by deciphering the partial data related to itself, using the encryption key in common with that of the card holder.

ABSTRACT OF THE DISCLOSURE

When a card holder who owns a payment card purchases merchandise from a seller via on-line communications through a network, partial data relative to other parties, i.e., the seller, a card manager, and a delivery service company, among the order data of the purchase, are encrypted by the terminal of the card holder using common cryptokeys which are effective only between the card holder and the other parties, and then transmitted through the terminal of the seller to the terminals 2~3 of the other parties. The other parties which have received the transmitted data decrypt the partial data relative to them using the common cryptokeys

DESCRIPTION

ELECTRONIC COMMERCE SYSTEM

TECHNICAL FIELD

The present invention relates to an electronic commerce system for allowing users or consumers to conduct commercial transactions via on-line communications on the Internet, personal computer communication networks, etc., and more particularly to an electronic commerce system which uses payment cards such as credit cards, debit cards, etc. for settling payments.

BACKGROUND ART

Recently, a growing number of users of computer networks including the Internet, personal computer communication networks, etc. are placing online orders to buy merchandise from sellers including electronic malls on the Internet and shops on the personal computer communication networks.

In order to conduct such an on-line commercial transaction, it is customary for the buyer to have readily available a payment card such as a credit card or a debit card, and transmits various data about the name, address, and telephone number of the buyer or card holder, the type, quantity, and other details of the merchandise to be purchased, and the card number and expiration date of the card, from the terminal of the card holder through the network to the seller. The seller carries out various processes to have the card manager (card company) authenticate the card holder, ship the merchandise or ask a delivery service company to ship the merchandise, and bill the card company for the price of the merchandise based on the data received by the terminal of the seller. The card company gives authentication of the card holder to the seller based on the data sent from the seller about the name, address, and telephone number of the card holder and the card number and expiration date of the card. The card company also withdraws funds from the account of the card holder to settle the payment based on the data of the price of the merchandise sent from the seller.

Electronic commerce systems for conducting such on-line commercial transactions have heretofore been open to various dangers including hacking (interception of communication data), cracking (substitution of communication data), and impersonation of the card holder, the merchant server (the terminal of the seller), and the acquirer gateway (the terminal of the card manager).

Of these attacks to the electronic commerce systems, the impersonation of the card holder can be prevented to a considerable extent by a database of card numbers which is possessed and managed by the card manager. Furthermore any damage which the card holder may suffer is relatively small even when a card holder is impersonated because an upper limit is usually established for the amount of money that can be settled by the card of the card holder.

However, the impersonation of the seller tends to cause a lot of damage since the false seller may possibly illegally collect and use card information such as of a large number of cards, expiration dates, etc.

In an attempt to solve the above problems, it has been the general practice to carry out communications using the identification number (ID number) and password of a card holder, or corresponding data, and to construct a so-called closed user group for preventing existing commercial transactions with the card from being affected even if the identification number and password are stolen. However, such a conventional system is not effective enough to solve the above problems.

Various efforts which have been proposed to eliminate the above drawbacks individually include encryption of communication data with a stream common-key cipher using DES (Data Encryption Standard), authentication with a public-key cipher such as the RSA system, etc. Nevertheless, there has not been constructed an electronic commerce system which is simple and versatile.

It is therefore an object of the present invention to provide an electronic commerce system which uses payment cards for settling payments via online communications with a simple and versatile system arrangement to avoid the danger of impersonation of sellers, etc. for secure online commercial transactions.

DISCLOSURE OF INVENTION

To accomplish the above object, there is provided in accordance with the present invention an electronic commerce system for conducting commercial transactions via online communications on a network between terminals of parties including at least a seller, a card holder who uses a payment card to purchase merchandise from the seller, and a card manager for managing payments made by the payment card, comprising means in the terminal of the card holder, for generating order data produced when the card holder purchases merchandise from said seller using the payment card, reproducing from the order data partial data with respect to the card holder and respective parties other than the card holder, for each of the respective parties, and encrypting the partial data which was reproduced for each of the respective parties with common cryptokeys which are effective only between the card holder and the respective parties other than the card holder, and then transmitting encrypted order data including the encrypted partial data through the terminal of the seller to the parties other than the card holder, means in the terminals of the parties other than the card holder, for decrypting only the encrypted partial data with respect to the parties other than the card holder, among the encrypted order data, using the respective common cryptokeys, means in the terminal of the card manager, for allowing commercial transactions, including issuance of an authentication of the card holder to the seller, to be made with respect to the card manager, based on the partial data decrypted by the terminal of the card manager, and means in the terminal of the seller, for allowing commercial transactions, including delivery of the merchandise, to be made with respect to the seller, based on the partial data decrypted by the terminal of the seller and the authentication of the card holder issued from the card manager.

The card holder who wishes to purchase merchandise from the seller using the payment card generates order data, and next reproduces from the order data partial data with respect to the card holder and respective parties other than the card holder, for each of the respective parties, thereby generating partial data. In addition, the card holder encrypts each of the partial data with respect to the card holder and the other parties using common cryptokeys effective only between the card holder and the parties other than the card holder. Such encrypted partial data is made into encrypted order data which is assembled from the partial data. The card holder then transmits the encrypted order data from the terminal of the card holder through the terminal of the seller to the terminals of the parties including the seller. The order data thus encrypted are securely protected from unauthorized access.

Each of the parties including the seller and the card manager, etc., who has received the encrypted order data, decrypts a part of them relative to itself using the common cryptokey shared by the card holder. It is unable to decrypt and comprehend other's encrypted data since each of the parties does not have a common cryptokey for decrypting the partial data relative to the other parties. Stated otherwise, each of the parties can comprehend details of the order data only within a range that is concerned with the party, and hence cannot steal any partial data that do not involve itself. The card manager effects commercial transactions related to itself, which include issuance of an authentication of the card holder to the seller, based on the partial data decrypted by the terminal of the card manager. The seller effects commercial transactions related to itself, which include delivery of the merchandise, based on the partial data decrypted by the terminal of the seller and the authentication of the card holder issued from the card manager. In this manner, electronic commercial transactions are conducted via online communications.

The security of the order data are maintained since the order data are encrypted before being transmitted. Each of the parties other than the card holder is supplied with minimum necessary data among the order data. Even if a third party impersonates the seller, the false seller is unable to access information involving the card manager, e.g., the card number and expiration date of the payment card, and hence can not achieve anything from the impersonation of the seller. Therefore the electronic commerce system is effective to ensure security of on-line commercial transactions through the network while eliminating the danger of illegal impersonation of the seller or other parties. The encrypted order data generated by the terminal of the card holder are transmitted through the terminal of the seller to the other parties. Therefore the card holder has only to transmit the encrypted order data only to the seller in purchasing merchandise via online communications. It is thus relatively simple to conduct online commercial transactions using the electronic commerce system.

The order data include data of a destination (which may not necessarily be the address of the card holder) of delivery of the merchandise, and the parties include a delivery service company.

In this case, the data of the destination are encrypted using only a common cryptokey which is effective only between the card holder and the delivery service company, and the delivery service company is allowed to deliver the merchandise based on the partial data, including the data of the destination, decrypted by the terminal of the delivery service company and instructions given from the seller. The privacy of the destination is protected since the data of the destination are comprehended only by the delivery service company.

The order data include data of a card number and expiration date of the payment card, and the data of the card number and expiration date are encrypted using only the common cryptokey effective only between the card holder and the card manager. Therefore the data of the card number and expiration date, which are the most important in settling payments for online commercial transactions using the payment card, are comprehended by the card manager only when the card manager decrypts the encrypted order data. Stated otherwise, any parties other than the card manager and the card holder are unable to know the data of the card number and expiration date of the payment card. As a consequence, security of the electronic commerce system is effectively maintained, and any unlawful impersonation by willful parties of the seller, which is the most dangerous act against online commercial transactions, is effectively prevented.

The common cryptokeys may be separately established and distributed between the card holder and other parties. Preferably, however, identifiers which are public and peculiar respectively to the parties other than the card holder may be entered into a secret private key peculiar to the card holder to generate the common cryptokeys which are effective only between the card holder and the parties other than the card holder, and an identifier which is public and peculiar to the card holder may be entered into respective secret private keys peculiar to the parties other than the card holder to generate the common cryptokeys which are effective only between the card holder and each of other parties. The identifier may comprise any attribute which is public and peculiar to each party, e.g., the name, address, mail addressor domain name on the network, or their combination of each party.

Consequently, each of the parties including the card holder enters the identifier of another party, with which a common cryptokey is to be shared, into the secret private key of its own to generate the common cryptokey. Therefore each party can generate the common cryptokey required for commercial transactions simply by entering identifier of the other party into its own secret private key without establishing and distributing the common cryptokey in advance. The electronic commerce system according to the present invention is thus highly simple and versatile. The security of communication data is reliably maintained while the communication data are being transmitted through the network since there is no need to distribute common cryptokeys in advance, so the safety of the electronic commerce system is high.

The above process of generating common cryptokeys is disclosed in "NON-PUBLIC KEY DISTRIBUTION/Advances in Cryptology: Proceedings of CRYPTO '82/Plenum Press, 1983, pp.231 - 236" by Rolf Blom, "An Optimal Class of Symmetric Key Generation Systems/Advances in Cryptology: EUROCRYPT '84/Springer LNCS 209, 1985, pp.335 - 338" by Rolf Blom, and Japanese patent publication No. 5-48980, for example, and hence will not be described in detail below.

Preferably, each of the parties communicates with other parties to which the encrypted order data are to be transmitted prior to the transmission of the encrypted order data for thereby confirming the other parties. Such advance confirmation of the parties is effective to prevent damages which would otherwise be caused by impersonation of the seller, the card manager, or the like. Therefore the safety of the electronic commerce system is further increased.

BRIEF DESCRIPTION OF DRAWINGS

FIG.1 is a block diagram of an electronic commerce system according to the present invention;

FIG.2 is a flowchart of a data processing sequence at a car holder in the electronic commerce system shown in FIG.1;

FIG.3 is a flowchart of data processing sequences at parties other than the card holder in the electronic commerce system shown in FIG.1.

BEST MODE FOR CARRYING OUT THE INVENTION

A preferred embodiment of the present invention is described below making reference to FIG.1 and FIG.2.

As shown in FIG. 1, an electronic commerce system according to the present invention comprises a terminal 1 of a card holder who owns a payment card (not shown) such as a credit card, a debit card, or the like, a terminal 2 of a seller, a terminal 3 of a card manager (card company) which manages payments by way of payment cards, and a terminal 4 of a delivery service company which delivers merchandise handled by the seller. The terminals 1, 2, 3, 4 are connected for communication with each other by a network 5 such as the Internet, a personal computer communication network, or the like. The card holder, the seller, the card manger, and the delivery service company are parties to an electronic commercial transaction described later on.

Each of the terminals 1, 2, 3, 4 comprises a computer machine such as a personal computer or the like. Each of the terminals 1, 2, 3, 4 contains a secret private key 6, which is a common cryptokey generation system for generating a common cryptokey for ciphertext communications between arbitrary parties, and an encryption/decryption system 7 for encrypting and decrypting communication data with the common cryptokey 6 as software or hardware implementations. These systems 6, 7 have previously been sent to the parties from a central organization (not shown) which issues cryptokeys and performs other tasks.

As can be seen from the articles by Rolf Blom and Japanese patent publication No.5-48980 referred to above, the secret private key 6 is peculiar to each of the parties, and generates a common cryptokey with respect to another party to communicate with when an identifier which is public and peculiar to each party, such as the name, address, or the like of the other party, is entered through each of the terminals 1, 2, 3, 4.

The encryption/decryption system 7 serves to encrypt communication data with the common cryptokey using known DES (Data Encryption Standard), or the like (at a transmission side for the communication data) and decrypt communication data which have been encrypted (at a reception side for the communication data).

An electronic commercial transaction is conducted using the above electronic commerce system as follows:

It is assumed that each of the parties communicates with another party to which encrypted order data (described later on) are to be transmitted through their terminals 1~4 over the Internet, the personal computer communication network, or the like, and that each of the parties between which to transmit encrypted order data has confirmed in advance that the other party legitimately exists, i.e., has authenticated the other party.

The card holder has acquired beforehand merchandise information of the seller through either communications between its own terminal 1 and the terminal 2 of the seller to see a home page of the seller, for example, or a browse of catalog data of the seller based on a recording medium such as a CD-ROM, a magazine, or the like.

The card holder asks the seller to send the data of an order form before purchasing merchandise from the seller. Alternatively, the card holder may obtain the data of an order form from a CD-ROM or the like.

Then the card holder enters order data to purchase the desired merchandise with its own payment card through the terminal 1 using the order form. As shown in FIG.2, the order data which are entered through the terminal 1 include the name, address, telephone number, and FAX number of the card holder, the card number and expiration date of the payment card owned by the card holder, the name, quantity, and item number of the merchandise, the amount due, the type of payment (installment, full payment, etc.), and the destination of delivery of the merchandise (including the name, address, etc. of the destination).

The order data are not limited to the above details, but may contain information necessary for the seller, the card manager, and the delivery service company to perform their tasks relative to a commercial transaction, e.g., identification by the seller of the card holder who has placed an order and details of the order, authentication of the card holder by the card manager, settlement of the amount due, delivery of the merchandise by the delivery service company, when the card holder is going to buy the merchandise using its own payment card.

After the above order data are entered, the card holder extracts predetermined partial data relative to the seller, the card manager, and the delivery service company from the order data, and duplicates the extracted partial data. The partial data related to the seller are duplicated, which specify the card holder and the details of the order, i.e., the name, address, telephone number, and FAX number of the card holder, the name, quantity, and item number of the merchandise, the amount due, and the type of payment, etc. The partial data relative to the card manager are duplicated, which authenticate the card holder and settles the payment, i.e., the name, address, telephone number, and FAX number of the card holder, the card number and expiration date of the payment card owned by the card holder, the item number of the merchandise, the amount due, and the type of payment, etc. The partial data relative to the delivery service company are duplicated, which are required to deliver the merchandise, i.e., the name, address, telephone number, and FAX number of the card holder, and the destination of delivery of the merchandise, etc.

A procedure to enable the card holder to extract and duplicate the above partial data, or a software program for automatically carrying out such a procedure has been sent to the card holder before the data of the order form have been sent from the seller to the card holder. Therefore, the card holder extracts and duplicates the above partial data according to the procedure or the software program which have been given to the card holder. The partial relative to the above parties are not limited to the data illustrated above, but some of the illustrated data may be dispensed with or additional data may be added thereto. For example, the data of the FAX number of the card holder may not be needed by any of those parties, the data of the item number of the merchandise may not be needed by the card manager due to the law and custom in the country in which the electronic commerce system is used, and the data of the destination of delivery of the merchandise may be needed by the seller.

The common cryptokeys for ciphertext communications between the card holder and the seller, the card manager, and the delivery service company are generated by entering respective identifiers of each of those parties into the secret private key 6 at the terminal 1 of the card holder.

The identifier of the delivery service company or information, e.g., the name of the delivery service company, required for the card holder to recognize the identifier of the delivery service company has been given to the card holder before the data of the order form have been sent from the seller to the card holder since the delivery service company is designated by the seller. The card holder has already recognized the identifiers of the seller and the card manager because the seller and the card manager have been designated by the card holder itself.

The card holder duplicates the partial data relative to the seller, the card manager, and the delivery service company from the order data, and generates the common cryptokeys for communications between the card holder and each of those parties. Then the card holder instructs the encryption/decryption system 7 to encrypt those partial data with the common cryptokeys, and transmits one set of communication data comprising encrypted order data including the encrypted partial data and the identifier of the card holder from the terminal 1 through the network 5 to the terminal 2 of the seller as indicated by the broken-line arrow "x" in FIG. 1. The identifier of the card holder which is transmitted together with the encrypted order data is not encrypted. The information (the name, address of the card holder, etc.) which enables the other parties to specify the identifier of the card holder may be transmitted together with the encrypted order data instead of the identifier of the card holder.

The communication data are securely protected from unauthorized access while in transmission through the network 5 since the encrypted order data, which make up a major part of the communication data, have been encrypted, any third parties which are not the seller, the card manager, and the delivery service company can not read the communication data.

The seller, who has received the communication data, i.e., the encrypted order data and the identifier of the card holder at its own terminal 2, generates the common cryptokey in common with the card holder by entering the identifier contained in the communication data into the secret private key 6'in the terminal 2. The seller decrypts the partial data relative to itself among the encrypted order data with the encryption/decryption system 7 in the terminal 2 as shown in FIG.3, by using the generated common cryptokey. The seller now acquires necessary data, i.e., the name, address, telephone number, and FAX number of the card holder, the name, quantity, and item number of the merchandise, the amount due, and the type of payment.

The partial data relative to the parties, i.e., the card manager and the delivery service company, other than the seller, have been encrypted with the common cryptokeys different from the common cryptokey for communication between the seller and the card holder. Consequently, the seller cannot decrypt the partial data relative to the card manager and the delivery service company, and hence cannot comprehend the card number and expiration date, which are data concerned with the card manager, and the destination of delivery of the merchandise, which is data concerned with the delivery service company.

Furthermore, the seller transmits the encrypted order data and the identifier of the card holder from the terminal 2 through the network 5 to the terminal 3 of the card manager as indicated by the broken-line arrow "y" in FIG. 1. While the seller may transmit all the received data to the card manager, the seller may transmit only the partial data relative to the card manager among the encrypted order data, together with the identifier of the card holder to the card manager.

The card manager, who has received the encrypted order data and the identifier of the card holder at its own terminal 3, generates the common cryptokey in common with the card holder by entering the identifier of the card holder into the secret private key 6 in the terminal 3. Then the card manager decrypts the partial data relative to itself among the encrypted order data with the encryption /decryption system 7 in the terminal 3 using the common cryptokey as shown in FIG.3. Therefore the card manager now acquires necessary data, i.e., the name, address, telephone number, and FAX number of the card holder, the card number and expiration date of the payment card owned by the card holder, the name, quantity, and item number of the merchandise, the amount due, and the type of payment. At this time, the card manager is unable to comprehend those data of the encrypted order data other than the partial data relative to itself, e.g., the destination of delivery of the merchandise, which is the data concerned with only the delivery service company.

The card manager, who has acquired the above data, authenticates the card holder i.e., determines whether the card holder is a legitimate card user or not, based on the data of the name, telephone number, the card number and expiration date of the payment card, etc. and transmits the result of authentication to the seller. If the card holder is a legitimate card user, then the card manager will carry out a process of withdrawing funds from the account of the card holder based on the data related to the amount due and the type of payment.

The seller, who has received the result of authentication from the card manager, transmits the encrypted partial data and the identifier of the card holder from the terminal 2 through the network 5 to the terminal 4 of the delivery service company as indicated by the broken-line arrow "z" in FIG.1 if the result of authentication indicates that the card holder is a legitimate card user. Then the seller transmits a request for delivery of the merchandise to the delivery service company based on the acquired partial data. If necessary, the seller lays in the merchandise. The seller may transmit only the partial data relative to the delivery service company among the encrypted order data together with the identifier of the card holder to the delivery service company.

The delivery service company, which has received the encrypted order data and the identifier of the card holder at its own terminal 4, generates the common cryptokey in common with the card holder by entering the identifier of the card holder into the secret private key 6 in the terminal 4. Then the delivery service company decrypts the partial data relative to itself among the encrypted order data with the encryption/decryption system 7 in the terminal 4 using the common cryptokey as shown in FIG.3. Therefore the delivery service company now acquires necessary data, i.e., the name, telephone number, and FAX number of the card holder, and the destination of delivery of the merchandise. At this time the delivery service company is unable to comprehend those data of the encrypted order data other than the partial data relative to the delivery service company, e.g., the card number and expiration date of the payment card.

The delivery service company, who has acquired the above data, carries out a process of delivering the merchandise to the destination based on the data and instructions from the seller.

In the above electronic commerce system, the partial data relative to the seller, the card manager, and the delivery service company, among the order data generated by the card holder, are encrypted using the common cryptokeys effective between the card holder and those parties, and the encrypted partial data are transmitted to the parties. Therefore the security of the order data is maintained while in transmission through the network 5. Each of the parties is able to acquire necessary data among the order data with the common cryptokey in common with the card holder. Stated otherwise, each of the parties can acquire those necessary data only. Therefore the seller and the delivery service company, for example, are unable to know the card number and expiration date of the payment card, which are the most important data for commercial transactions using the payment card. Even if a third party impersonates the seller or the delivery service company, the third party can not achieve anything from the impersonating act because the third party is unable to comprehend the important data of the card number and expiration date of the payment card. Accordingly the electronic commerce system is effective to prevent any third parties from impersonating the seller or the delivery service company.

Each of the parties including the card holder communicates with other parties to which encrypted order data are to be transmitted prior to the transmission of the encrypted order data for thereby confirming the other parties. Therefore the electronic commerce system is also capable of preventing any third parties from impersonating the card manager as well as the seller or the delivery service company.

The inventor of the present application conducted a test on the electronic commerce system to make various attacks on the electronic commerce system. As a result it was found that the electronic commerce system was capable of withstanding those attacks.

The data of the destination cannot be comprehended by the seller and the card manager because the data of the destination of delivery of the merchandise are encrypted using only the common cryptokey common to the card holder and the delivery service company in the embodiment. Thus the privacy of that person is protected when the card holders sends the purchased merchandise to a person other than the card holder.

When the card holder buys merchandise the encrypted order data are transmitted through the terminal 2 of the seller to the seller, the card manager, and the delivery service company. Then the card holder has only to transmit the encrypted order data to the terminal 2 of the seller, so is able to purchase merchandise through online communications easily.

The partial data relative to the seller, the card manager, and the delivery service company respectively are encrypted by the card holder, and the common cryptokeys used by the seller, the card manager, and the delivery service company to decrypt the partial data are generated simply when each of the parties enters the identifier of a certain party the secret private key in its terminal 1-4. Accordingly it is not necessary for the parties to establish common cryptokeys or receive common cryptokeys distributed from a central organization each time a commercial transaction is to be made. The parties thus find it simple to conduct commercial transactions via on-line communications.

The electronic commerce system according to the present invention, therefore, is secure, simple, and versatile.

The electronic commerce system may be constructed without the participation of a delivery service company, or may be constructed so as to include a gateway manager such as an Internet service provider, a key authentication office, etc. as parties to the electronic commerce system while the parties to the electronic commerce system include a delivery service company in this embodiment.

Each of the parties generates a common cryptokey when it enters the identifier of a certain party into the secret private key in its terminal in the embodiment. However, the parties may use separately established common cryptokeys, or may receive a common cryptokey distributed from a central organization.

INDUSTRIAL APPLICABILITY

The system according to the present invention is available preferably as a commercial transaction system using payment cards, including credit cards, debit cards, etc. via on-line communications with the terminals e.g. personal computers, etc. on a network such as the Internet, a personal computer communication network, or the like.

CLAIMS

1. (Amended) An electronic commerce system for conducting commercial transactions via online communications on a network between terminals of parties including at least a seller, a card holder who uses a payment card to purchase merchandise from the seller, and a card manager for managing payments made by the payment card, comprising:

means in the terminal of the card holder, for generating order data produced when said card holder purchases merchandise from said seller using the payment card, reproducing from said order data partial data with respect to the card holder and respective parties other than the card holder, for each of said respective parties, and encrypting said partial data which was reproduced for each of said respective parties with common cryptokeys which are effective only between the card holder and said respective parties other than the card holder, and then transmitting encrypted order data including the encrypted partial data through the terminal of the seller to the parties other than the card holder;

means in the terminals of the parties other than the card holder, for decrypting only the encrypted partial data with respect to the parties other than the card holder, among said encrypted order data, using the respective common cryptokeys;

means in the terminal of the card manager, for allowing commercial transactions, including issuance of an authentication of said card holder to the seller, to be made with respect to said card manager, based on the partial data decrypted by the terminal of said card manager; and means in the terminal of the seller, for allowing commercial transactions, including delivery of the merchandise, to be made with respect to said seller, based on the partial data decrypted by the terminal of said seller and the authentication of said card holder issued from said card manager.

2. An electronic commerce system according to claim 1, wherein said order data include data of a destination of delivery of the merchandise, and said parties include a delivery service company, said data of the destination being encrypted using only a common cryptokey which is effective only between the card holder and said delivery service company, further comprising:

means in a terminal of the delivery service company, for allowing the delivery service company to deliver the merchandise based on the partial data, including the data of the destination, decrypted by the terminal of the delivery service company and instructions given from said seller.

3. An electronic commerce system according to claim 1 or 2, wherein said order data include data of a card number and expiration date of the payment card, and said data of the card number and expiration date are encrypted using only the common cryptokey which is effective only between the card holder and said card manager.

4. An electronic commerce system according to claim 1 or 2, further comprising:

means in the terminal of the card holder, for entering identifiers which are public and peculiar respectively to the parties other than the card holder into a secret private key peculiar to the card holder to generate said common cryptokeys which are effective only between the card holder and the parties other than the card holder; and

means in the terminals of the parties other than the card holder, for entering an identifier which is public and peculiar to the card holder into respective secret private keys peculiar to the parties other than the card holder to generate said common cryptokeys which are effective only between the card holder and the parties other than the card holder.

5. An electronic commerce system according to claim 1 or 2, wherein each of said parties communicates with other parties to which the encrypted order data are to be transmitted prior to the transmission of the encrypted order data for thereby confirming the other parties.

FIG. 1

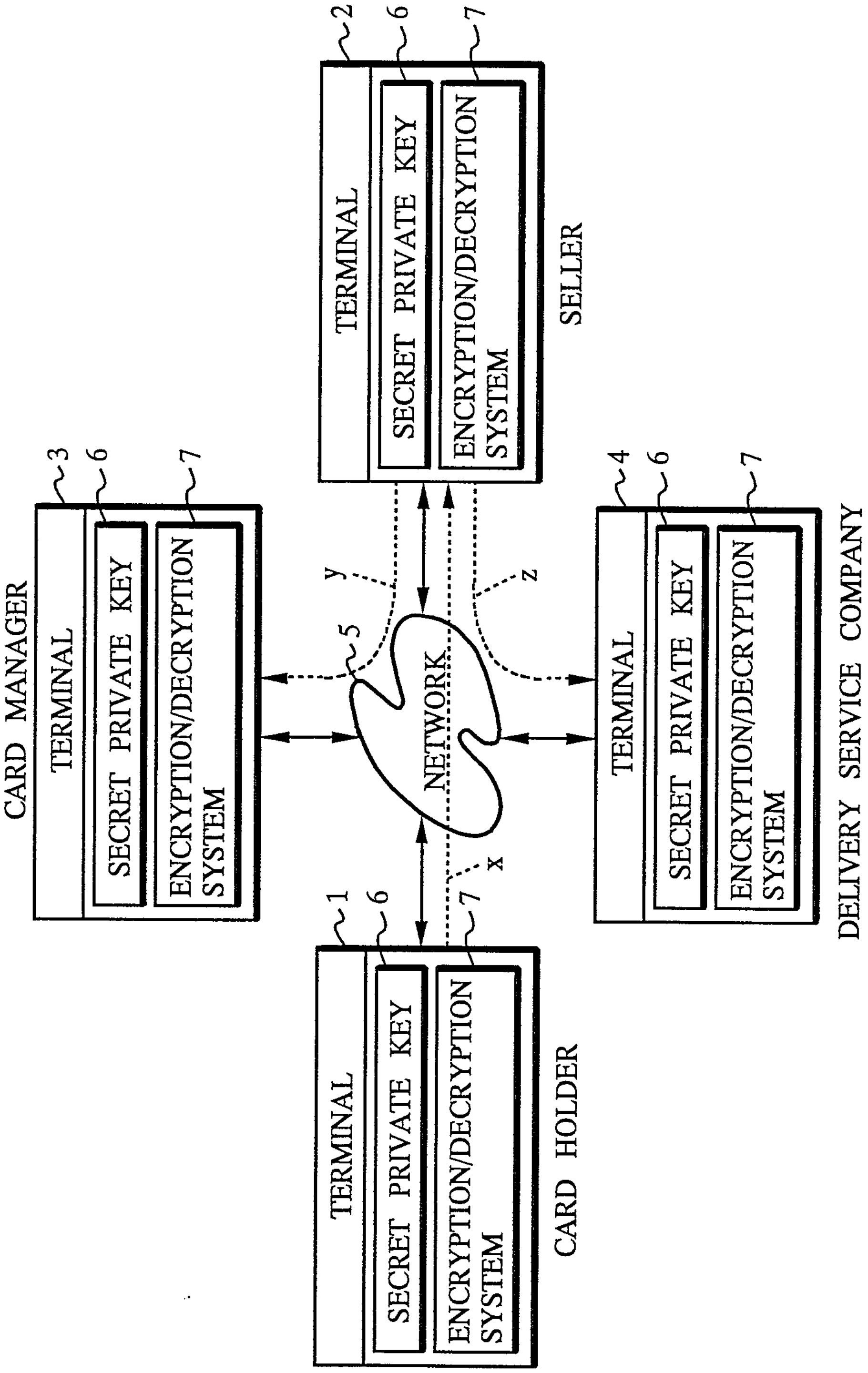

CARD MANAGER
TERMINAL
SECRET PRIVATE KEY
ENCRYPTION/DECRYPTION SYSTEM
3
6
7
SELLER
TERMINAL
SECRET PRIVATE KEY
ENCRYPTION/DECRYPTION SYSTEM
2
6
7
NETWORK
5
x
y
z
CARD HOLDER
TERMINAL
SECRET PRIVATE KEY
ENCRYPTION/DECRYPTION SYSTEM
1
6
7
DELIVERY SERVICE COMPANY
TERMINAL
SECRET PRIVATE KEY
ENCRYPTION/DECRYPTION SYSTEM
4
6
7

FIG. 2

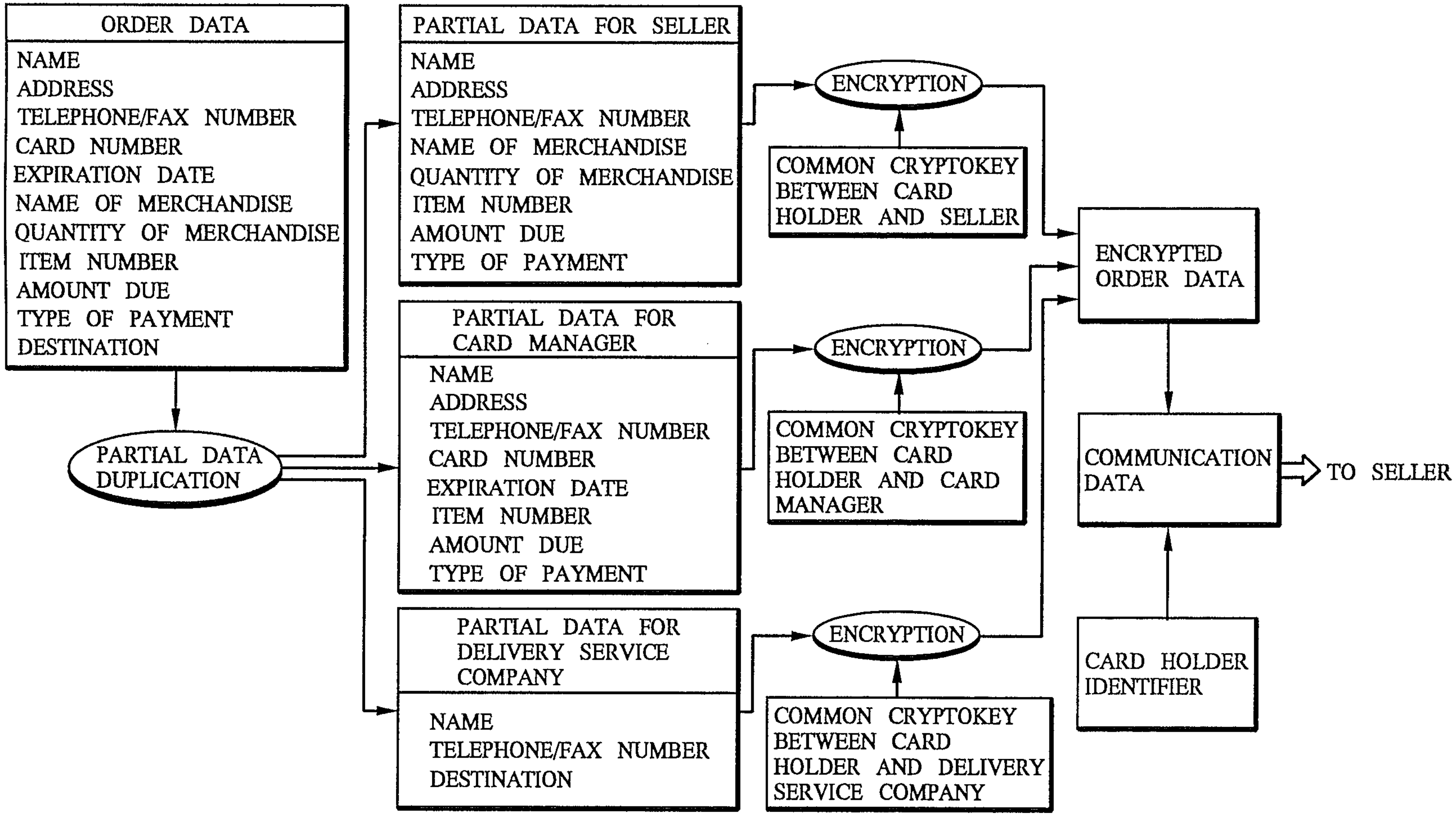
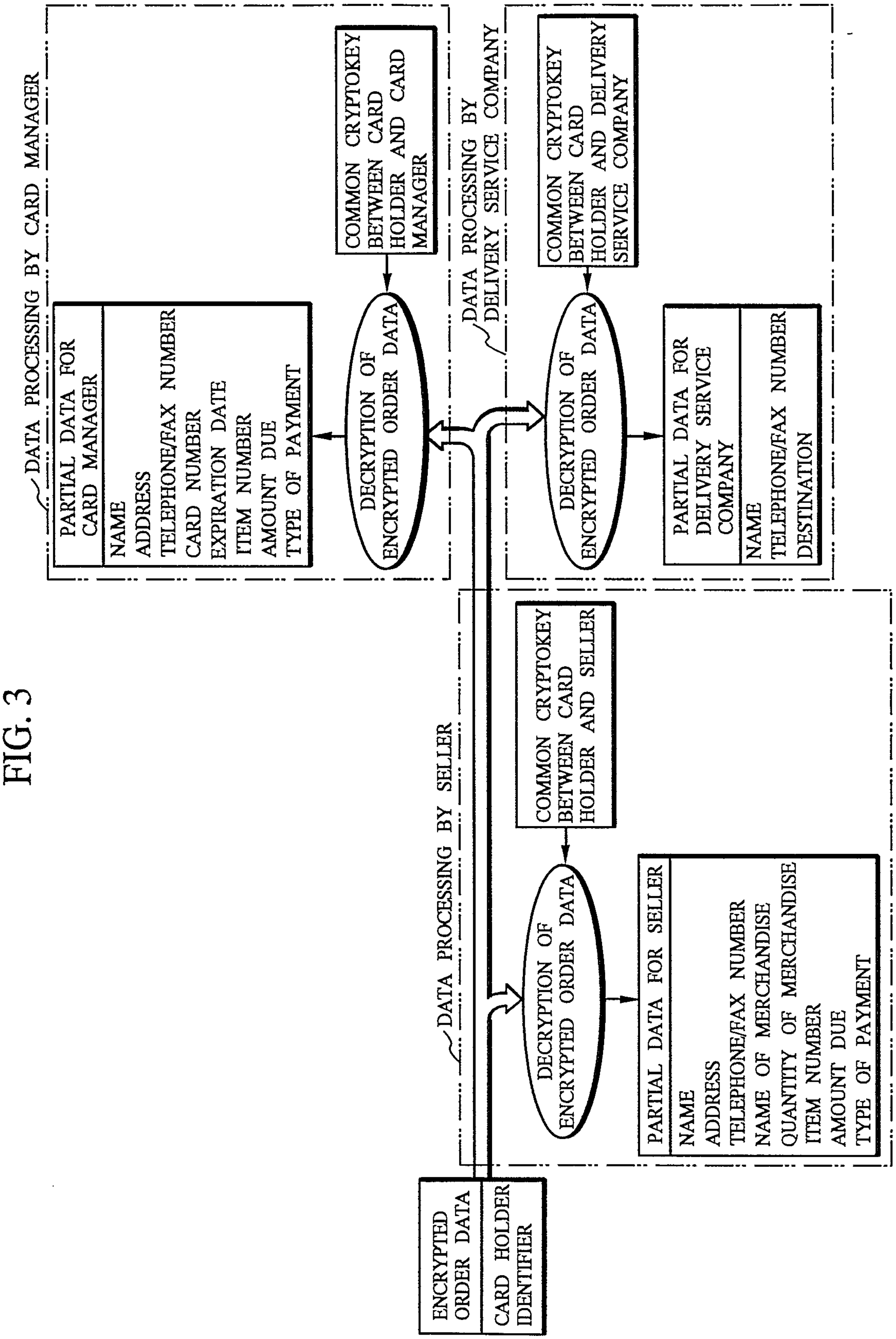
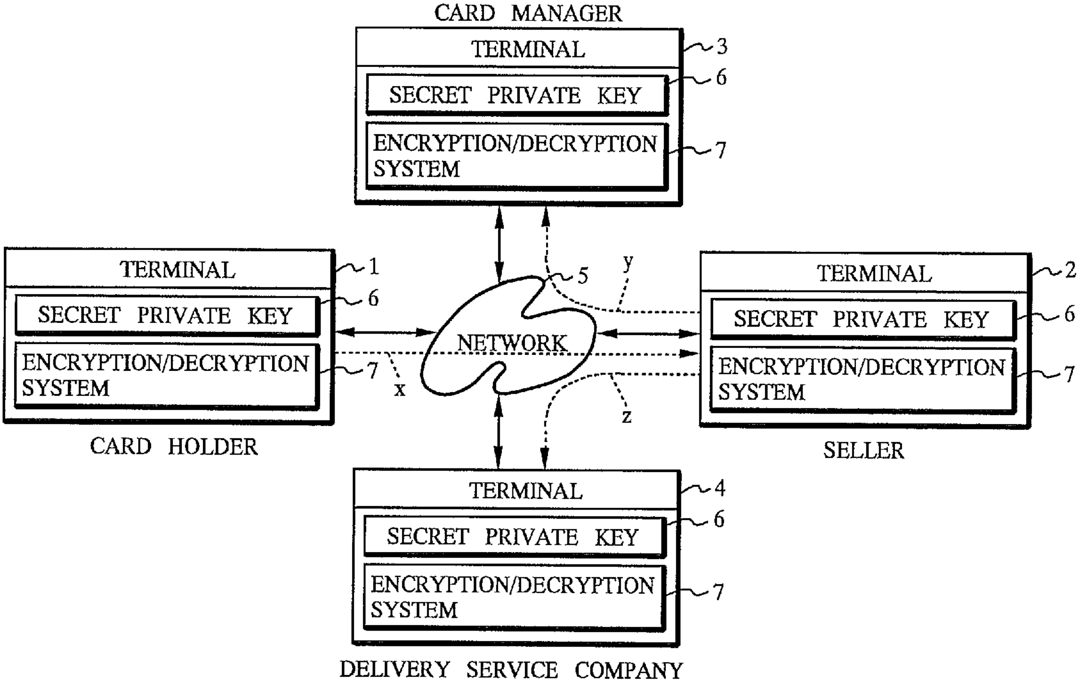

ORDER DATA
NAME
ADDRESS
TELEPHONE/FAX NUMBER
CARD NUMBER
EXPIRATION DATE
NAME OF MERCHANDISE
QUANTITY OF MERCHANDISE
ITEM NUMBER
AMOUNT DUE
TYPE OF PAYMENT
DESTINATION
PARTIAL DATA DUPLICATION
PARTIAL DATA FOR SELLER
NAME
ADDRESS
TELEPHONE/FAX NUMBER
NAME OF MERCHANDISE
QUANTITY OF MERCHANDISE
ITEM NUMBER
AMOUNT DUE
TYPE OF PAYMENT
PARTIAL DATA FOR CARD MANAGER
NAME
ADDRESS
TELEPHONE/FAX NUMBER
CARD NUMBER
EXPIRATION DATE
ITEM NUMBER
AMOUNT DUE
TYPE OF PAYMENT
PARTIAL DATA FOR DELIVERY SERVICE COMPANY
NAME
TELEPHONE/FAX NUMBER
DESTINATION
ENCRYPTION
COMMON CRYPTOKEY BETWEEN CARD HOLDER AND SELLER
ENCRYPTION
COMMON CRYPTOKEY BETWEEN CARD HOLDER AND CARD MANAGER
ENCRYPTION
COMMON CRYPTOKEY BETWEEN CARD HOLDER AND DELIVERY SERVICE COMPANY
ENCRYPTED ORDER DATA
COMMUNICATION DATA
TO SELLER
CARD HOLDER IDENTIFIER

FIG. 3


ENCRYPTED ORDER DATA
CARD HOLDER IDENTIFIER
DATA PROCESSING BY CARD MANAGER
PARTIAL DATA FOR CARD MANAGER
NAME
ADDRESS
TELEPHONE/FAX NUMBER
CARD NUMBER
EXPIRATION DATE
ITEM NUMBER
AMOUNT DUE
TYPE OF PAYMENT
DECRYPTION OF ENCRYPTED ORDER DATA
COMMON CRYPTOKEY BETWEEN CARD HOLDER AND CARD MANAGER
DATA PROCESSING BY DELIVERY SERVICE COMPANY
COMMON CRYPTOKEY BETWEEN CARD HOLDER AND DELIVERY SERVICE COMPANY
DECRYPTION OF ENCRYPTED ORDER DATA
PARTIAL DATA FOR DELIVERY SERVICE COMPANY
NAME
TELEPHONE/FAX NUMBER
DESTINATION
DATA PROCESSING BY SELLER
COMMON CRYPTOKEY BETWEEN CARD HOLDER AND SELLER
DECRYPTION OF ENCRYPTED ORDER DATA
PARTIAL DATA FOR SELLER
NAME
ADDRESS
TELEPHONE/FAX NUMBER
NAME OF MERCHANDISE
QUANTITY OF MERCHANDISE
ITEM NUMBER
AMOUNT DUE
TYPE OF PAYMENT


CARD MANAGER
TERMINAL
3
SECRET PRIVATE KEY
6
ENCRYPTION/DECRYPTION SYSTEM
7
TERMINAL
1
SECRET PRIVATE KEY
6
ENCRYPTION/DECRYPTION SYSTEM
7
CARD HOLDER
x
NETWORK
5
y
z
TERMINAL
2
SECRET PRIVATE KEY
6
ENCRYPTION/DECRYPTION SYSTEM
7
SELLER
TERMINAL
4
SECRET PRIVATE KEY
6
ENCRYPTION/DECRYPTION SYSTEM
7
DELIVERY SERVICE COMPANY